

Docket No.: P2001,0201

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : THORSTEN BÖKER ET AL.

Filed : CONCURRENTLY HEREWITH

Title : DATA CARRIER

CLAIM FOR PRIORITY

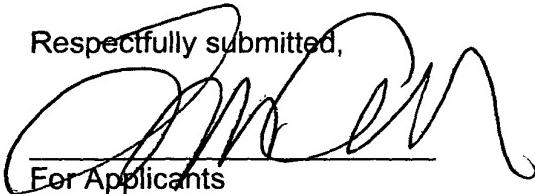
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119,
based upon the German Patent Application 101 13 531.9, filed March 20, 2001.

A certified copy of the above-mentioned foreign patent application is being submitted
herewith.

Respectfully submitted,


For Applicants

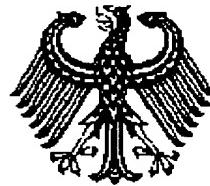
LAURENCE A. GREENBERG
REG. NO. 29,308

Date: September 22, 2003

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

/kf

BUNDESREPUBLIK DEUTSCHLAND



Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 101 13 531.9

Anmeldetag: 20. März 2001

Anmelder/Inhaber: Infineon Technologies AG,
München/DE

Bezeichnung: Datenträger

IPC: G 06 F 12/14

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 28. August 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

A handwritten signature in black ink, appearing to begin with the letters 'St'.

Stromberg

Beschreibung

Datenträger

5 Die Erfindung betrifft einen Datenträger mit einem nicht-flüchtigen elektronischen Speicher zur Aufnahme großer Datenmengen. Solche Datenträger werden verwendet, um große Datenmengen speichern zu können, wobei die Datenträger auch als wechselbare Medien geeignet sind. In einer verhältnismäßig
10 neuen Anwendung werden wechselbare Datenträger dieser Art dazu verwendet, beispielsweise aus dem Internet geladene Musikdateien oder elektronische Bücher zu speichern. In einem möglichen Anwendungsfall dient ein normaler PC als Ladestation, durch den die Dateien beschafft und auf dem Datenträger gespeichert werden. Anschließend sind die gespeicherten Daten
15 auf einem transportablen Wiedergabegerät abspielbar, beispielsweise eine MP3-Datei auf einem mobilen MP3-Player.

20 In anderen Anwendungen dienen solche Datenträger als Ersatz für Disketten oder Wechselseitplatten. In diesem Fall sind oftmals sensible Daten gespeichert, die vor dem Zugriff unberechtigter Dritter zu schützen sind. Dafür kann die Datei vor dem Speichern auf dem Datenträger verschlüsselt und sodann in verschlüsselter Form auf dem Datenträger gespeichert werden.
15 Dies bedeutet allerdings einen erhöhten Aufwand, so daß in vielen Fällen auf die Verschlüsselung verzichtet wird.

Aufgabe der Erfindung ist es daher, einen Datenträger anzugeben, der zur Aufnahme großer Datenmengen geeignet ist und da-
30 bei eine hohe Sicherheit für die gespeicherten Daten ermöglicht.

35 Diese Aufgabe wird durch einen Datenträger der eingangs genannten Art gelöst, der dadurch gekennzeichnet ist, daß ein zur Durchführung kryptographischer Operationen geeigneter Mikrocontroller vorgesehen und der Zugriff auf den Speicher nur über den Mikrocontroller möglich ist.

Durch die erfindungsgemäße Gestaltung des Datenträgers ist somit sichergestellt, daß Daten immer verschlüsselt in dem Speicher abgelegt sind.

5

In einer vorteilhaften Ausgestaltung der Erfindung erfolgt über den Mikrocontroller eine Authentifizierung des Benutzers. Während durch die verschlüsselte Speicherung die Daten für einen Benutzer schützbar sind, kann mit der Authentifizierung des Benutzers von Seiten der Datenquelle sichergestellt werden, daß Daten nur an einen bestimmten Benutzer abgegeben werden.

10

In einer bevorzugten Ausgestaltung ist der Speicher größer als 1 MB und in Form einer Chipkarte ausgestaltet.

15

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels näher beschrieben. Die Figur beschreibt einen erfindungsgemäßen Datenträger in einer Anordnung zum Laden von Daten aus dem Internet.

20

Ein Datenträger 1 besitzt einen nicht-flüchtigen Massenspeicher 2 mit einer Speicherkapazität von typischerweise größer als 1 MB. Für den Speicherbaustein sind verschiedene Technologien einsetzbar, beispielsweise Flash, OTP, MTP oder ähnliche. Außerdem weist der Datenträger, der als Chipkarte ausgestaltet ist, einen Kryptocontroller 3 auf, der Standardverschlüsselungsmethoden anwenden kann, vorzugsweise RSA oder elliptische Kurven. Der Datenträger 1 ist mit einer Ladestation 4 verbunden. Die Verbindung kann über elektrische Kontaktflächen oder kontaktlos über eine Antenne erfolgen. Als Ladestation 4 können spezielle Geräte vorgesehen sein oder ein normaler PC, der eine entsprechende Schnittstelle zur Kommunikation mit dem Datenträger 1 vorsieht. Die Ladestation 4 wiederum ist mit dem Internet 5 verbindbar. Vorteilhaft ist, wenn die Ladestation 4 ein Mobilfunkgerät ist, das eine drahtlose Kommunikation mit dem Internet 5 herstellen kann.

25

30

35

Somit ist der erfindungsgemäße Datenträger besonders flexibel einsetzbar.

Durch den Mikrocontroller 3 können Sicherheitsmaßnahmen flexibel vorgesehen werden. So übernimmt der Mikrocontroller die Identifizierung eines Kunden gegenüber einem Dienstanbieter im Internet und den Abrechnungsvorgang wie eine EC- oder Geldkarte. Der Speicher 2 nimmt sodann die heruntergeladenen Daten auf, wobei die Daten verschlüsselt im Speicher abgelegt sind.

In einer abgewandelten Anwendung werden verschlüsselte Daten beim Herunterladen durch den Mikrocontroller 3 entschlüsselt, so daß sie dem Benutzer zugänglich sind. Dabei sind sowohl die Schlüssel selbst wie ein Zertifikat zur optimalen Absicherung des Zugriffs auf die Daten in dem Datenträger gespeichert.

Bei der Ausgestaltung der Sicherheitsmechanismen kann auf sämtliche aus dem Stand der Technik bekannte Maßnahmen zurückgegriffen werden, da diese aufgrund der flexiblen Möglichkeiten durch den Mikrocontroller 3 allesamt einsetzbar sind. Zukünftigen Entwicklungen bei der Verschlüsselungstechnologie ist somit Rechnung getragen.

Die Sicherheit auf einer solchen Karte übertrifft diejenige der CD oder auch der DVD und ermöglicht das „Digitale Rights Management“ (DRM) im Rahmen von e-commerce.

Patentansprüche

1. Datenträger mit

einem nicht-flüchtigen elektronischen Speicher (2) zur Auf-

5 nahme großer Datenmengen,

dadurch gekennzeichnet, daß

ein zur Durchführung kryptographischer Operationen geeigneter Mikrocontroller (3) vorgesehen und der Zugriff auf den Speicher (2) nur über den Mikrocontroller (3) möglich ist.

10

2. Datenträger nach Anspruch 1,

dadurch gekennzeichnet, daß

die Speicherkapazität des Speichers (2) größer als 1 MByte ist.

15

3. Datenträger nach Anspruch 1,

dadurch gekennzeichnet, daß der Datenträger (1) ein wechselbarer Datenträger ist.

20

4. Datenträger nach Anspruch 1 oder 3,

dadurch gekennzeichnet, daß

der Datenträger in der Form einer Chipkarte ausgestaltet ist.

25 5. Datenträger nach einem der Ansprüche 1 bis 4,

dadurch gekennzeichnet, daß

vor der Speicherung von Daten in dem Speicher (2) eine Authentifizierung des Benutzers unter Verwendung des Mikrocontrollers (3) erfolgt.

30

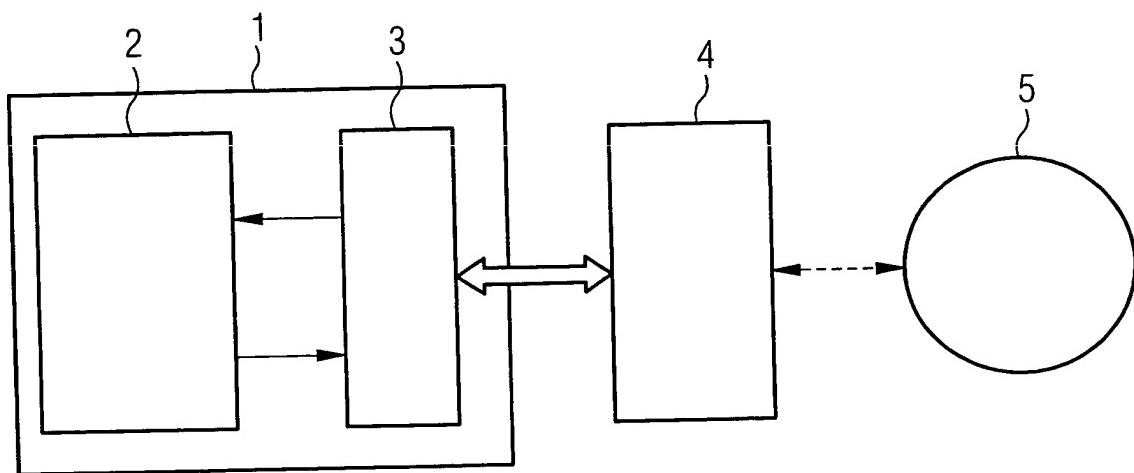
Zusammenfassung

Datenträger

- 5 Die Erfindung betrifft einen Datenträger mit einem nicht-flüchtigen elektronischen Speicher (2) zur Aufnahme großer Datenmengen. Dieser Datenträger ist dadurch gekennzeichnet,
daß ein zur Durchführung kryptographischer Operationen geeigneter Mikrocontroller (3) vorgesehen ist und der Zugriff auf
10 den Speicher (2) nur über den Mikrocontroller möglich ist.
Durch diese Anordnung ist einerseits ein größtmöglicher
15 Schutz für die gespeicherten Daten erreicht als auch eine Möglichkeit gegeben, den Benutzer gegenüber einem Diensteanbieter, von dem zu speichernde Daten stammen, zu authentifizieren und eine Abrechnung zwischen den Parteien zu ermöglichen.

Bezugszeichenliste

- 1 Datenträger
- 2 Massenspeicher
- 5 3 Mikrocontroller
- 4 Ladestation
- 5 Internet



(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
26. September 2002 (26.09.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/075505 A2

(51) Internationale Patentklassifikation: G06F 1/00

[DE/DE]; Albrecht-Dürer-Str. 3, 85579 Neubiberg

(21) Internationales Aktenzeichen: PCT/DE02/00540

(DE); SEDLAK, Holger [DE/DE]; Neumünster 10a.

(22) Internationales Anmeldedatum:

14. Februar 2002 (14.02.2002)

85658 Egmatting (DE); HAMMERSCHMITT, Jürgen

(25) Einreichungssprache:

Deutsch

[DE/DE]; Schwabenstr. 25c, 85521 Ottobrunn (DE);

(26) Veröffentlichungssprache:

Deutsch

WINKLER, Otto [DE/DE]; Zaun 55, 84332 Hebertsfelden (DE).

(30) Angaben zur Priorität:

101 13 531.9 20. März 2001 (20.03.2001) DE

(74) Anwalt: EPPING, HERMANN & FISCHER; Ridlerstr.

(71) Anmelder (*für alle Bestimmungsstaaten mit Ausnahme von US*): INFINEON TECHNOLOGIES AG [DE/DE];
St-Martin-Str. 53, 81669 München (DE).

55, 80339 München (DE).

(72) Erfinder; und

(81) Bestimmungsstaaten (*national*): BR, CA, CN, IL, IN, JP,

(75) Erfinder/Anmelder (*nur für US*): BÖKER, Thorsten

KR, MX, RU, UA, US.

(84) Bestimmungsstaaten (*regional*): europäisches Patent (AT,
BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE, TR).

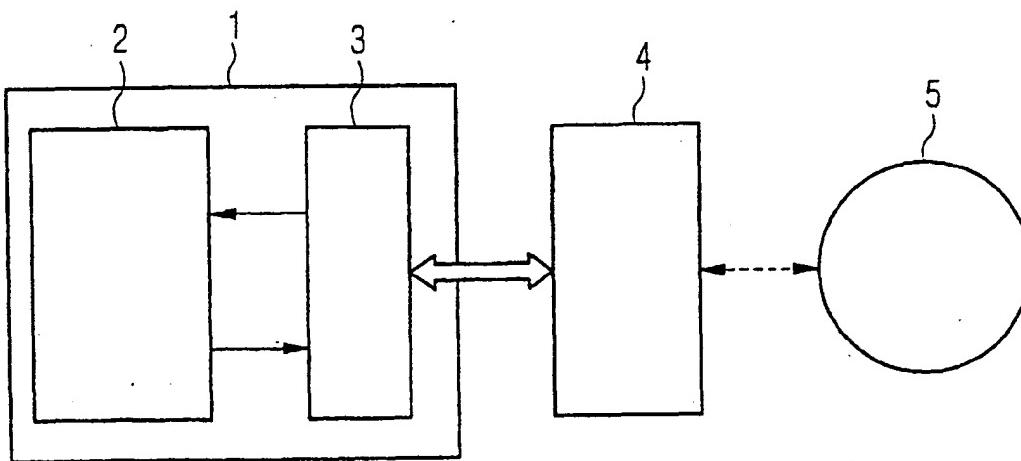
Veröffentlicht:

— ohne internationalen Recherchenbericht und erneut zu
veröffentlichen nach Erhalt des Berichts

[Fortsetzung auf der nächsten Seite]

(54) Titel: DATA CARRIER

(54) Bezeichnung: DATENTRÄGER



WO 02/075505 A2

(57) Abstract: The invention relates to a data carrier comprising a non-volatile electronic memory (2) for receiving large amounts of data and a microcontroller (3) which is suitable for carrying out cryptographic operations, whereby access to the memory (2) is only possible via the microcontroller (3). Said inventive data carrier is characterised in that an authentication of the user with respect to a data source takes place before data is stored in the memory (2) using said microcontroller (3).

(57) Zusammenfassung: Die Erfindung betrifft einen Datenträger mit einem nichtflüchtigen elektronischen Speicher (2) zur Aufnahme großer Datenmengen und einem zur Durchführung kryptographischer Operationen geeigneten Mikrocontroller (3), wobei der Zugriff auf den Speicher (2) nur über den Mikrocontroller (3) möglich ist. Der erfindungsgemäße Datenträger ist dadurch gekennzeichnet, dass vor der Speicherung von Daten in dem Speicher (2) eine Authentifizierung des Benutzers gegenüber einer Datenquelle unter Verwendung des Mikrocontrollers (3) erfolgt.



Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Docket # P2004,0201

Applic. # _____

Applicant: Thorsten Böker el al.

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100 Fax: (954) 925-1101